



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,948	03/18/2004	Toshikazu Yasue	HAS-101	5164
24956 7590 01/14/2009 MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C. 1800 DIAGONAL ROAD SUITE 370 ALEXANDRIA, VA 22314				
EXAMINER				
MAL, KEVIN S				
ART UNIT		PAPER NUMBER		
2456				
MAIL DATE		DELIVERY MODE		
01/14/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/802,948

Applicant(s)

YASUE ET AL.

Examiner

KEVIN S. MAI

Art Unit

2456

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 December 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 and 3-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 and 3-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-8508)
Paper No(s)/Mail Date 11/26/08
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This Office Action has been issued in response to Applicant's Request for Continued Examination filed December 23, 2008.
2. Claim 2 has been canceled. Claims 1, 3-9 and 11-16 have been amended. Claims 1 and 3-16 have been examined and are pending.

Response to Arguments

4. Applicant's arguments with respect to claims 1 and 3-16 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 1, 3-7 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pub. No. 2003/0174718 to Sampath et al. (hereinafter “Sampath”) and further in view of US Pub. No. 2003/0221016 to Jouppi et al. (hereinafter “Jouppi”).

8. **As to claim 1**, Sampath discloses **a network authentication apparatus comprising: a network interface unit connected with a network and that transmits/receives a packet** (Paragraph [0011] of Sampath discloses a network device for network communications, the device includes at least one data port interface. The data port interface supporting at least one data port transmitting and receiving data and a CPU interface); **a packet relay unit that relays a received packet in accordance with a destination address of the received packet** (Figure 1 of Sampath discloses that apparatus of Sampath’s invention. Then in paragraph [0014] it is disclosed that one of the functionalities of that invention is to discard, forward or modify packets based upon the filtering done. Therefore since the apparatus disclosed by Sampath is capable of forwarding packets it reads upon the limitation above); **and** Sampath does not explicitly disclose **a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and**

only the interface ID part of the source IPv6 address extracted from the received packet

Sampath discloses a filtering processing unit that extracts one or more of a destination MAC address and a destination IPv6 address and a source MAC address and source IPv6 address and determining whether to relay a received packet or discard a packet in accordance with the extracted fields.

Paragraph [0014] of Sampath discloses running packets through a faster filtering processor to obtain a selective filter action. The packets are discarded, forwarded or modified based upon the filtering, it is seen that in order to select a filter action according to the fields the fields must have been extracted from the incoming packet. Then paragraph [0051] discloses a field table that specifies the fields of interest for the filter. The field table is clarified in paragraph [0052] to contain three portions which are described in TABLE 3. In TABLE 3 it is seen that fields F1 and F2 can be any of the Source MAC address, Destination MAC address, Source IP address and L4 Source Port, Destination IP address and L4 Port, or a user defined 16 bit field. These two fields are seen to be the same as those in applicant's invention. As to the IP addresses being IPv6, paragraph [0042] discloses the fields include Ethernet and IPv4 fields, as well as IPv6 field. Then as to the source IPv6 interface ID being considered, it is seen that Sampath discloses considering the source IPv6 address which is seen to include the interface ID. Thus when considering the source IPv6 address, the interface id is automatically considered.

Sampath does not explicitly disclose only using the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

It would have been obvious to one of ordinary skill in the art at the time of invention to combine filtering packets according to the destination MAC/IP address and source MAC address as disclosed by Sampath, with filtering packets according to their interface ID as disclosed by Jouppi. One of ordinary skill in the art would have been motivated to combine to improve security as well as makes processing easier and faster (paragraph [0031] of Jouppi).

9. **As to claim 3, Sampath-Jouppi discloses the network authentication apparatus as claimed in claim 1, wherein the filtering processing unit further comprises: a filtering information storage unit that stores at least one or more of the destination MAC address and the destination IPv6 address and the source MAC address, that stores the interface ID part of the source IPv6 address and that stores judgment information representing whether to relay or discard, in association with each other** (Paragraph [0039] of Sampath discloses the filter logic works by masking the portions of the packet that the filter is not interested in. Thus after masking is done a search key is generated that will be used to search for a match in the rules table. This rules table is seen to contain the destination MAC address and destination IPv6 address and source MAC address or source IPv6 address, because based on the selections of fields F1 and F2 the rules table would then consist of the corresponding addresses. That is if F1 and F2 were assigned to be the Destination MAC address and the Source IP address respectively, then the search key would be composed of the Destination MAC address and the Source IP address. Then since the search key is used to match against the entries in the rules table, the rules table must contain the Destination MAC address and Source IP addresses also. As to the judgment information, paragraphs [0036] and [0037] disclose that the results are

obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that the rules table also contains the judgment information); and

a processing unit that compares:

(a) one or more of the destination MAC address and the destination IPv6 address and the source MAC address, and (b) only the interface ID part of the source IPv6 address extracted from in the received packet with (a) one or more of the destination MAC address and the destination IPv6 address and the source MAC address, and (b) only the interface ID part of the source IPv6 address stored in the filtering information storage unit, wherein when the addresses and ID parts match with each other, determining whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with (a) one or more of the destination MAC address or the destination IPv6 address and the source MAC address, and (b) the interface ID part of the source IPv6 address (Paragraph [0036] of Sampath discloses a Fast Filtering Processor that is used for the filtering of incoming packets. As disclosed above the filtering process involves masking the bits that are not relevant to the search and thus creating a search key that is composed of the fields chosen in the fields table. Thus if F1 and F2 were assigned to be the Destination MAC address and the Source IP address respectively, the processor would be matching those against the entries in the rules tables (paragraph [0039]). As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the

CPU. Thus it is seen that if a match is found the results are taken from the rules table determining if the packet is discarded or forwarded).

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sampath and Jouppi it is seen that it would be obvious for Sampath's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

10. **As to claim 4, Sampath-Jouppi discloses the network authentication apparatus as claimed in claim 1, wherein the filtering processing unit comprises:**
a MAC filtering unit that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the destination MAC address and the source MAC address contained in the received packet (Paragraph [0014] of Sampath discloses that a packet is discarded, forwarded or modified based upon the filtering. Then in paragraphs [0051] and [0052] and TABLE 3 it is disclosed that the fields of interest for the filter can be selected and among the choices are the Destination MAC address and Source MAC address. Thus Sampath's Fast Filtering Processor (paragraph [0036]) can use the MAC address for filtering and determining whether to forward or discard packets); **and**
an IP filtering unit that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the destination MAC address and only the

interface ID part of the source IPv6 address extracted from the received packet (Paragraph [0014] of Sampath discloses that a packet is discarded, forwarded or modified based upon the filtering. Then in paragraphs [0051] and [0052] and TABLE 3 it is disclosed that the fields of interest for the filter can be selected and among the choices are the Destination MAC address and Source IP address. Thus Sampath's Fast Filtering Processor (paragraph [0036]) can use the IP address for filtering and determining whether to forward or discard packets).

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

11. **As to claim 5, Sampath-Jouppi discloses the network authentication apparatus as claimed in claim 4,**

wherein the filtering processing unit further comprises:

a filtering information storage unit that stores at least the destination MAC address and the source MAC address or only the interface ID part of the source IPv6 address and, the judgment information representing whether to relay or discard, in association with each other (Paragraph [0039] of Sampath discloses the filter logic works by masking the portions of the packet that the filter is not interested in. Thus after masking is done a search key is generated that will be used to search for a match in the rules table. This rules table is seen to contain the destination MAC address and, source MAC address or source IPv6 address, because based on the

selections of fields F1 and F2 the rules table would then consist of the corresponding addresses. That is if F1 and F2 were assigned to be the Destination MAC address and the Source IP address respectively, then the search key would be composed of the Destination MAC address and the Source IP address. Then since the search key is used to match against the entries in the rules table, the rules table must contain the Destination MAC address and Source IP addresses also. As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that the rules table also contains the judgment information).

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sampath and Jouppi it is seen that it would be obvious for Sampath's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

12. **As to claim 6, Sampath-Jouppi discloses the network authentication apparatus as claimed in claim 4,**

wherein the MAC filtering unit further comprises:

a MAC filtering information storage unit that stores the destination MAC address and the source MAC address and the judgment information representing whether relay or discard,

in association with each other (Paragraph [0039] of Sampath discloses the filter logic works by masking the portions of the packet that the filter is not interested in. Thus after masking is done a search key is generated that will be used to search for a match in the rules table. This rules table is seen to contain the destination MAC address and, source MAC address or source IPv6 address, because based on the selections of fields F1 and F2 the rules table would then consist of the corresponding addresses. That is if F1 and F2 were assigned to be the Destination MAC address and the Source MAC address respectively, then the search key would be composed of the Destination MAC address and the Source MAC address. Then since the search key is used to match against the entries in the rules table, the rules table must contain the Destination MAC address and Source MAC addresses also. As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that the rules table also contains the judgment information); **and**

wherein the IP filtering unit further comprises:

an IP filtering information storage unit that stores the destination MAC address and only the interface ID part of the source IPv6 address and the judgment information representing whether to relay or discard, in association with each other (Paragraph [0039] of Sampath discloses the filter logic works by masking the portions of the packet that the filter is not interested in. Thus after masking is done a search key is generated that will be used to search for a match in the rules table. This rules table is seen to contain the destination MAC address and, source MAC address or source IPv6 address, because based on the selections of fields F1 and F2 the rules table would then consist of the corresponding addresses. That is if F1 and F2

were assigned to be the Destination MAC address and the Source IP address respectively, then the search key would be composed of the Destination MAC address and the Source IP address. Then since the search key is used to match against the entries in the rules table, the rules table must contain the Destination MAC address and Source IP addresses also. As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that the rules table also contains the judgment information).

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sampath and Jouppi it is seen that it would be obvious for Sampath's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

13. As to claim 7, Sampath-Jouppi discloses **the network authentication apparatus as claimed in claim 6,**
wherein the MAC filtering unit compares the destination MAC address and the source MAC address contained in the received packet with the destination MAC address and the source MAC address stored in the MAC filtering information storage unit, and when the addresses match with each other, determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information

associated with the destination MAC address and the source MAC address (As Sampath disclosed above in claim 6 the filtering process involves masking the bits that are not relevant to the search and thus creating a search key that is composed of the fields chosen in the fields table. Thus if F1 and F2 were assigned to be the Destination MAC address and the Source MAC address respectively, the processor would be matching those against the entries in the rules tables (paragraph [0039]). As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that if a match is found the results are taken from the rules table determining if the packet is discarded or forwarded), **and**

wherein the IP filtering unit compares the destination MAC address and only the interface ID part of the source IPv6 address contained in the received packet with the destination MAC address and only the interface ID part of the source IPv6 address stored in the IP filtering information storage unit, and when the addresses and interface ID parts match with each other, determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with the destination MAC address and only the interface ID part of the source IPv6 address (As Sampath disclosed above in claim 6 the filtering process involves masking the bits that are not relevant to the search and thus creating a search key that is composed of the fields chosen in the fields table. Thus if F1 and F2 were assigned to be the Destination MAC address and the Source IP address respectively, the processor would be matching those against the entries in the rules tables (paragraph [0039]). As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering

logic decides if the packet is discarded or sent to the CPU. Thus it is seen that if a match is found the results are taken from the rules table determining if the packet is discarded or forwarded).

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sampath and Jouppi it is seen that it would be obvious for Sampath's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

14. Claims 1, 3-8 and 11 – 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pub. No. 2002/0016858 to Sawada et al. (hereinafter “Sawada”) and further in view of Jouppi.

15. **As to Claim 1**, Sawada discloses **a network authentication apparatus comprising: a network interface unit connected with a network and that transmits/receives a packet** (Figure 1 of Sawada discloses network interface units connected with the network. Then paragraph [0072] discloses that the network interfaces perform packet sending and receiving); **a packet relay unit that relays a received packet in accordance with a destination address of the received packet** (Paragraph [0073] of Sawada discloses a packet forwarding unit that performs packet forwarding); **and**

a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with;
one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and

only the interface ID part of the source IPv6 address extracted from the received packet
(Paragraph [0114] of Sawada discloses a filtering unit containing a packet processor. The packet processor discards a packet or transfers it according to the information contained in the filtering table. Then paragraphs [0116] and [0139] disclose the filtering table containing judgment information, MAC address information and IP address information. Wherein containing IP address information is seen to include the IPv6 interface ID because the IP address inherently includes the interface ID).

Sawada does not explicitly disclose only using the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

It would have been obvious to one of ordinary skill in the art at the time of invention to combine filtering packets according to the destination MAC/IP address and source MAC address as disclosed by Sawada, with filtering packets according to their interface ID as disclosed by

Jouppi. One of ordinary skill in the art would have been motivated to combine to improve security as well as makes processing easier and faster (paragraph [0031] of Jouppi).

16. As to Claim 3, Sawada-Jouppi discloses the network authentication apparatus as claimed in claim 1, wherein the filtering processing unit further comprises:
a filtering information storage unit that stores at least one or more of the destination MAC address and the destination IPv6 address and the source MAC address, that stores the interface ID part of the source IPv6 address and that stores judgment information representing whether to relay or discard, in association with each other (Figure 12 of Sawada discloses the filtering table containing destination address information, source address information, and judgment information); and
a processing unit that compares:
(a) one or more of the destination MAC address and the destination IPv6 address and the source MAC address, and (b) only the interface ID part of the source IPv6 address extracted from in the received packet with (a) one or more of the destination MAC address and the destination IPv6 address and the source MAC address, and (b) only the interface ID part of the source IPv6 address stored in the filtering information storage unit, wherein when the addresses and ID parts match with each other, determining whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with (a) one or more of the destination MAC address or the destination IPv6 address and the source MAC address, and (b) the interface ID part of the source IPv6 address (Paragraph [0116] of Sawada discloses the forward/discard flag

field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Thus it is seen that judgment is made on matches made in the table).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sawada and Jouppi it is seen that it would be obvious for Sawada's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

17. **As to Claim 4, Sawada-Jouppi discloses the network authentication apparatus as claimed in claim 1, wherein the filtering processing unit comprises:**
a MAC filtering unit that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the destination MAC address and the source MAC address contained in the received packet (Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Paragraph [0139] discloses the filtering table containing MAC address information. Thus it is seen filtering is done based off the MAC address); **and**

an IP filtering unit that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the destination MAC address and only the interface ID part of the source IPv6 address extracted from the received packet (Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Paragraph [0139] discloses the filtering table containing IP and MAC address information. Thus it is seen filtering is done based off the IP and MAC address).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

18. **As to Claim 5**, Sawada-Jouppi discloses **the network authentication apparatus as claimed in claim 4**,
wherein the filtering processing unit further comprises:
a filtering information storage unit that stores at least the destination MAC address and the source MAC address or only the interface ID part of the source IPv6 address and, the judgment information representing whether to relay or discard, in association with each other (Figure 12 of Sawada discloses the filtering table containing destination address information, source address information, and judgment information).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sawada and Jouppi it is seen that it would be obvious for Sawada's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

19. **As to Claim 6, Sawada-Jouppi discloses the network authentication apparatus as claimed in claim 4,**

wherein the MAC filtering unit further comprises:

a MAC filtering information storage unit that stores the destination MAC address and the source MAC address and the judgment information representing whether relay or discard, in association with each other (Figure 12 of Sawada discloses the filtering table containing destination address information, source address information, and judgment information.

Paragraph [0139] discloses the filtering table containing MAC address information); **and**

wherein the IP filtering unit further comprises:

an IP filtering information storage unit that stores the destination MAC address and only the interface ID part of the source IPv6 address and the judgment information representing whether to relay or discard, in association with each other (Figure 12 of Sawada discloses the filtering table containing destination address information, source address

information, and judgment information. Paragraph [0139] discloses the filtering table containing IP and MAC address information).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sawada and Jouppi it is seen that it would be obvious for Sawada's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

20. **As to Claim 7, Sawada-Jouppi discloses the network authentication apparatus as claimed in claim 6,**
wherein the MAC filtering unit compares the destination MAC address and the source MAC address contained in the received packet with the destination MAC address and the source MAC address stored in the MAC filtering information storage unit, and when the addresses match with each other, determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with the destination MAC address and the source MAC address (Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Thus it is seen that

judgment is made on matches made in the table. Paragraph [0139] discloses the filtering table containing MAC address information), **and**

wherein the IP filtering unit compares the destination MAC address and only the interface ID part of the source IPv6 address contained in the received packet with the destination MAC address and only the interface ID part of the source IPv6 address stored in the IP filtering information storage unit, and when the addresses and interface ID parts match with each other, determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with the destination MAC address and only the interface ID part of the source IPv6 address

(Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Thus it is seen that judgment is made on matches made in the table. Paragraph [0139] discloses the filtering table containing IP address information).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sawada and Jouppi it is seen that it would be obvious for Sawada's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

21. **As to Claim 8**, Sawada-Jouppi discloses **the network authentication apparatus as claimed in claim 1, further comprising:**
an authentication unit that receives an authentication request from an arbitrary information terminal device connected to the network interface unit via a network and that executes authentication based on predetermined information received from the arbitrary information terminal device (Paragraph [0084] of Sawada discloses a server for authentication that judges whether a terminal user that is attempting a connection is authorized to do so. A terminal user is authenticated by user ID and password).

22. **As to Claim 11**, Sawada discloses **a network authentication system comprising:**
an authentication server that receives an authentication request from an arbitrary information terminal device connected via a network, and that executes authentication based on predetermined information received from the arbitrary information terminal device (Paragraph [0084] of Sawada discloses a server for authentication that judges whether a terminal user that is attempting a connection is authorized to do so. A terminal user is authenticated by user ID and password); **and**
a network node device connected to the network and that relays a packet received from the network,
wherein the network node device comprises:
a network interface unit connected with the network and that transmits/receives a packet;
(Figure 1 of Sawada discloses network interface units connected with the network. Then paragraph [0072] discloses that the network interfaces perform packet sending and receiving);

a packet relay unit that relays a received packet in accordance with a destination address of the received packet (Paragraph [0073] of Sawada discloses a packet forwarding unit that

performs packet forwarding); **and**

a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with;

one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and

only the interface ID part of the source IPv6 address received from the received packet (Paragraph [0114] of Sawada discloses a filtering unit containing a packet processor. The packet processor discards a packet or transfers it according to the information contained in the filtering table. Then paragraphs [0116] and [0139] disclose the filtering table containing judgment information, MAC address information and IP address information), **and**

wherein the filtering processing unit relays only a packet addressed to the authentication server to the packet relay unit, of packets sent from an arbitrary information terminal device that is not authenticated by the authentication server (This limitation is read to mean that only packets that are addressed to the authentication server and are from a device that has not yet been authenticated get sent to the authentication server. Paragraph [0169] of Sawada discloses to gain authentication the user inputs user ID and password to their terminal. It is seen that doing this action is the only way of contacting the authentication server and as such can only

be done when the user is not yet authenticated. A user is unable to log in again after already being logged in before logging out. Thus it is seen that only packets that have not yet been authenticated arrive at the authentication server).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

23. **As to Claim 12, Sawada-Jouppi discloses the network authentication system as claimed in claim 11,**

wherein the filtering processing unit of the network node device further comprises:

a filtering information storage unit that stores at least one or more of the destination MAC address and the destination IPv6 address and the source MAC address, that stores the interface ID part of the source IPv6 address, and that stores judgment information

representing whether to relay or discard in association with each other (Figure 12 of Sawada discloses the filtering table containing destination address information, source address information, and judgment information); and

a processing unit that compares:

(a) one or more of the destination MAC address and the destination IPv6 address and the source MAC address (b) only the interface ID part of the source IPv6 address extracted from the received packet with (a) one or more of the destination MAC address and the

destination IPv6 address and the source MAC address and (b) only the interface ID part of the source IPv6 address stored in the filtering information storage unit, wherein when the addresses and **ID parts** match with each other, determining whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with (a) **one or more of** the destination MAC address and the destination IPv6 address **and the source MAC address and (b) the interface ID part of the source IPv6 address** (Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Thus it is seen that judgment is made on matches made in the table).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sawada and Jouppi it is seen that it would be obvious for Sawada's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

24. **As to Claim 13, Sawada-Jouppi discloses the network authentication system as claimed in claim 12,**

wherein the authentication server includes an instruction issuing unit that adds an instruction of the arbitrary information terminal device when the arbitrary information

terminal device is authenticated (Paragraphs [0104] – [0105] of Sawada disclose after a user has been authenticated a directive packet to change state of the user is sent),
wherein the network node device includes a change unit that newly registers only the interface ID part of the source IPv6 address of the arbitrary information terminal device as the interface ID part of the source IPv6 address into the filtering information storage unit together with the judgment information representing relay in accordance with an instruction from the authentication server (Paragraph [0105] of Sawada disclose updating the learned table by looking for the MAC address of the user and then designating it to the connected state. Then paragraph [0106] discloses that because it is a connected state packets sent from it are then forwarded. Thus it is seen to be having the addresses and judgment information), **and wherein the filtering processing unit relays a packet sent from the arbitrary information terminal device authenticated by the authentication server, to the packet relay unit** (Paragraph [0073] of Sawada discloses a packet forwarding unit that performs packet forwarding).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

25. **As to Claim 14, Sawada-Jouppi discloses the network authentication system as claimed in claim 11,**

wherein the filtering processing unit of the network node device further comprises:

a MAC filtering unit that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the destination MAC address and the source MAC address contained in the received packet (Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Paragraph [0139] discloses the filtering table containing MAC address information. Thus it is seen filtering is done based off the MAC address); **and**

an IP filtering unit that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the destination MAC address and only interface ID part of the source IPv6 address contained in the received packet (Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Paragraph [0139] discloses the filtering table containing IP and MAC address information. Thus it is seen filtering is done based off the IP and MAC address).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

26. **As to Claim 15**, Sawada-Jouppi discloses **the network authentication system as claimed in claim 14**,
wherein the filtering processing unit of the network node device further comprises:
a filtering information storage unit for that stores at least the destination MAC address and the source MAC address or only the interface ID part of the source IPv6 address, and judgment information representing relay or discard in association with each other (Figure 12 of Sawada discloses the filtering table containing destination address information, source address information, and judgment information. Paragraph [0139] discloses the filtering table containing MAC and IP address information),
wherein the MAC filtering unit compares the destination MAC address and the source MAC address contained in the received packet with the destination MAC address and the source MAC address stored in the filtering information storage unit, and when the addresses match with each other, determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with the destination MAC address and the source MAC address (Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Thus it is seen that judgment is made on matches made in the table. Paragraph [0139] discloses the filtering table containing MAC address information), **and**

wherein the IP filtering unit compares destination MAC address and only the interface ID part of the source IPv6 address contained in the received packet with the destination MAC address and only the interface ID part of the source IPv6 address stored in the filtering information storage unit, and

wherein when the addresses and interface ID parts match with each other, determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with the destination MAC address and only the interface ID part of the source IPv6 address (Paragraph [0116] of Sawada discloses the forward/discard flag field contains information to indicate whether to forward or discard a packet received whose destination address and source address match the destination address condition and the source address condition. Thus it is seen that judgment is made on matches made in the table. Paragraph [0139] discloses the filtering table containing IP address information).

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

27. **As to Claim 16, Sawada discloses a switch apparatus comprising:**

plural network interface units connected with a network and that transmit/receive packets
(Figure 1 of Sawada discloses network interface units connected with the network. Then paragraph [0072] discloses that the network interfaces perform packet sending and receiving);
a packet relay unit that relays a received packet between the plural network interface units in accordance with a destination address of the received packet (Paragraph [0073] of Sawada discloses a packet forwarding unit that performs packet forwarding); **and**
a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet switch unit or discard the packet in accordance with;
one or more of a destination MAC address and the destination IPv6 address and the source MAC address; and
only the interface ID part of the source IPv6 address extracted from the received packet
(Paragraph (Paragraph [0114] of Sawada discloses a filtering unit containing a packet processor. The packet processor discards a packet or transfers it according to the information contained in the filtering table. Then paragraphs [0116] and [0139] disclose the filtering table containing judgment information, MAC address information and IP address information); **and**
an authentication unit that executes authentication based on predetermined information received from an arbitrary information terminal device connected to one of the network interface units via the network (Paragraph [0084] of Sawada discloses a server for

authentication that judges whether a terminal user that is attempting a connection is authorized to do so. A terminal user is authenticated by user ID and password),

wherein the filtering processing unit determines a condition for a determination of whether to relay or discard based on the authentication result by the authentication unit (Paragraph [0073] of Sawada discloses a packet forwarding unit that performs packet forwarding),

Sawada does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

28. Claims 8, 9, and 11 – 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sampath-Jouppi and further in view of U.S. Pat. No. 6442588 to Clark et al. (hereinafter “Clark”).

29. **As to claim 8**, Sampath-Jouppi discloses the invention as claimed as described in claim 1. Sampath-Jouppi does not explicitly disclose **an authentication unit that receives an authentication request from an arbitrary information terminal device connected to the network interface unit via a network and that executes authentication based on predetermined information received from the arbitrary information terminal device.**

However, Clark discloses this (Column 6 lines 15 – 25 of Clark disclose a user’s authentication request being forwarded to an authentication server for processing. The

authentication server then checks the user's ID and password received from the user with its own database. The user's ID and password are seen to be predetermined information related to the terminal device).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the apparatus of claim 1 as disclosed by Sampath, with having an authentication unit for receiving authentication requests as disclosed by Clark. One of ordinary skill at the time the invention was made would have been motivated to combine to provide security for a network by preventing unauthorized access (column lines 34 – 40 of Clark).

30. As to **claim 9**, Sampath-Jouppi-Clark discloses the invention as claimed as described in claim 8, **wherein the authentication unit comprises an authentication information storage unit that stores a user ID, password, and only the interface ID part of the source IPv6 address or MAC address in association with each other, and performs authentication by comparing a user ID, password, and only the interface ID part of the source IPv6 address or MAC address received from the arbitrary information terminal device with the user ID, password, and only the interface ID part of the source IPv6 address or MAC address stored in the authentication information storage unit** (Column 4 lines 35 - 41 of Clark disclose a dynamic filtering firewall that includes memory in which the user ID and current IP address currently assigned to the user is stored. The IP address is seen to inherently contain the IPv6 interface ID as disclosed by the applicant the interface ID is part of the IP address (paragraph 11 of applicant). As to containing the password, column 7 lines 55 - 60 disclose a profile that may be created for each subscriber which includes the subscriber's ID, password and

permission levels. Then it discloses that this information would be transmitted to the state tables of the dynamic filtering firewall. Thus the table is seen to hold the user ID, password and IP interface ID. As for performing authentication, column 7 lines 13 - 20 disclose routing requests to the dynamic firewall filter to determine if the subscriber has been authenticated. It then explains if the subscriber's user ID and originating address are contained in the DFF then the communication is allowed. As for also using the password in this comparison, column 7 lines 60 - 64 disclose that under the scenario where the profile is also part of the information in the state tables the customer profile would be checked each time the subscriber tried to access a service. Since the profile includes the password, it is seen that the comparison includes the password).

Examiner recites the same rationale to combine used in claim 8.

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sampath and Jouppi it is seen that it would be obvious for Sampath's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

31. **As to claim 11**, Sampath discloses a **network authentication system comprising:**

Sampath does not explicitly disclose **an authentication server that receives an authentication request from an arbitrary information terminal device connected via a network, and that**

executes authentication based on predetermined information received from the arbitrary information terminal device; and

However, Clark discloses this (Column 6 lines 15 – 25 of Clark disclose a user's authentication request being forwarded to an authentication server for processing. The authentication server then checks the user's ID and password received from the user with its own database. The user's ID and password are seen to be predetermined information related to the terminal device)

Examiner recites the same rationale to combine used in claim 8.

Sampath discloses **a network node device connected to the network and that relays a packet received from the network** (Paragraph [0011] of Sampath discloses a network device for network communications that includes a data port interface for transmitting and receiving data); **wherein the network node device comprises:**

a network interface unit connected with the network and that transmits/receives a packet; (Paragraph [0011] of Sampath discloses a network device for network communications, the device includes at least one data port interface. The data port interface supporting at least one data port transmitting and receiving data and a CPU interface);

a packet relay unit that relays a received packet in accordance with a destination address of the received packet (Figure 1 of Sampath discloses that apparatus of Sampath's invention.

Then in paragraph [0014] it is disclosed that one of the functionalities of that invention is to discard, forward or modify packets based upon the filtering done. Therefore since the apparatus disclosed by Sampath is capable of forwarding packets reads upon the limitation above); **and**

a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with;
one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and
only the interface ID part of the source IPv6 address received from the received packet

(Paragraph [0014] of Sampath discloses running packets through a faster filtering processor to obtain a selective filter action. The packets are discarded, forwarded or modified based upon the filtering. Then paragraph [0051] discloses a field table that specifies the fields of interest for the filter. The field table is clarified in paragraph [0052] to contain three portions which are described in TABLE 3. In TABLE 3 it is seen that fields F1 and F2 can be any of the Source MAC address, Destination MAC address, Source IP address and L4 Source Port, Destination IP address and L4 Port, or a user defined 16 bit field. These two fields are seen to be the same as those in applicant's invention. As to the IP addresses being IPv6, paragraph [0042] discloses the fields include Ethernet and IPv4 fields, as well as IPv6 field);

Sampath does not explicitly disclose **wherein the filtering processing unit relays only a packet addressed to the authentication server to the packet relay unit, of packets sent from an arbitrary information terminal device that is not authenticated by the authentication server.**

However, Clark discloses this (This limitation is read to mean that only packets that are addressed to the authentication server and are from a device that has not yet been authenticated get sent to the authentication server. Figure 4A of Clark discloses how a subscriber dials in to connect; they dial into a third party which then queries them for their user ID and password, then the third party sends an authentication request for the subscriber to the authentication server to be authenticated. It is seen that only through this process can packets even be sent to the authorization server. Thus it is seen that only packets that have not yet being authenticated can be sent to the authentication server).

Examiner recites the same rationale to combine used in claim 8.

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

32. **As to claim 12**, Sampath-Jouppi-Clark discloses the invention as claimed as described in claim 11,

wherein the filtering processing unit of the network node device further comprises:

a filtering information storage unit that stores at least one or more of the destination MAC address and the destination IPv6 address and the source MAC address, that stores the interface ID part of the source IPv6 address, and that stores judgment information representing whether to relay or discard in association with each other (Paragraph [0039] of

Sampath discloses the filter logic works by masking the portions of the packet that the filter is not interested in. Thus after masking is done a search key is generated that will be used to search for a match in the rules table. This rules table is seen to contain the destination MAC address and, source MAC address or source IPv6 address, because based on the selections of fields F1 and F2 the rules table would then consist of the corresponding addresses. That is if F1 and F2 were assigned to be the Destination MAC address and the Source IP address respectively, then the search key would be composed of the Destination MAC address and the Source IP address. Then since the search key is used to match against the entries in the rules table, the rules table must contain the Destination MAC address and Source IP addresses also. As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that the rules table also contains the judgment information); and a processing unit that compares:

(a) one or more of the destination MAC address and the destination IPv6 address and the source MAC address (b) only the interface ID part of the source IPv6 address extracted from the received packet with (a) one or more of the destination MAC address and the destination IPv6 address and the source MAC address and (b) only the interface ID part of the source IPv6 address stored in the filtering information storage unit, wherein when the addresses and ID parts match with each other, determining whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with (a) one or more of the destination MAC address and the destination IPv6 address and the source MAC address and (b) the interface ID part

of the source IPv6 address (Paragraph [0036] of Sampath discloses a Fast Filtering Processor that is used for the filtering of incoming packets. As disclosed above the filtering process involves masking the bits that are not relevant to the search and thus creating a search key that is composed of the fields chosen in the fields table. Thus if F1 and F2 were assigned to be the Destination MAC address and the Source IP address respectively, the processor would be matching those against the entries in the rules tables (paragraph [0039]). As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that if a match is found the results are taken from the rules table determining if the packet is discarded or forwarded).

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

In view of the combination of Sampath and Jouppi it is seen that it would be obvious for Sampath's invention to now only store the interface ID.

Examiner recites the same rationale to combine used in claim 1.

33. **As to claim 13**, Sampath-Jouppi-Clark discloses the invention as claimed as described in claim 12,

wherein the authentication server includes an instruction issuing unit that adds an instruction of the arbitrary information terminal device when the arbitrary information

terminal device is authenticated (Column 4 lines 47 – 53 of Clark disclose the dynamic filtering firewall maintaining a dynamic table of currently authenticated end-user IP addresses. Then column 6 lines 54 – 55 disclose the dynamic filtering firewall updating its state table to reflect that a subscriber has been authenticated. This is seen as having a unit for addition of information when devices are authenticated);

wherein the network node device includes a change unit that newly registers only the interface ID part of the source IPv6 address of the arbitrary information terminal device as the interface ID part of the source IPv6 address into the filtering information storage unit together with the judgment information representing relay in accordance with an instruction from the authentication server (Column 4 lines 47 – 53 of Clark disclose the dynamic filtering firewall maintaining a dynamic table of currently authenticated end-user IP addresses. Then column 6 lines 54 – 55 disclose the dynamic filtering firewall updating its state table to reflect that a subscriber has been authenticated. As to the information that is updated, column 4 lines 35 - 41 of Clark disclose a dynamic filtering firewall that includes memory in which the user ID and current IP address currently assigned to the user is stored. The judgment information is also in the table; column 7 lines 55 - 60 disclose a profile that may be created for each subscriber which includes the subscriber's ID, password and permission levels. The permission levels are seen to be judgment information. Thus it is seen that the dynamic filtering firewall maintains the table by registering the address and judgment information); **and wherein the filtering processing unit relays a packet sent from the arbitrary information terminal device authenticated by the authentication server, to the packet relay unit** (Figure 6A of Clark discloses a sample of a subscriber requesting information, as seen in step 614 the

dynamic filtering firewall checks to see if the IP address is marked as authenticated. If it is authenticated the communication is permitted and thus the packet would be forwarded).

Examiner recites the same rationale to combine used in claim 8.

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

34. **As to claim 14**, Sampath-Jouppi-Clark discloses the invention as claimed as described in claim 11,

wherein the filtering processing unit of the network node device further comprises:

a MAC filtering unit that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the destination MAC address and the source MAC address contained in the received packet (Paragraph [0014] of Sampath discloses that a packet is discarded, forwarded or modified based upon the filtering. Then in paragraphs [0051] and [0052] and TABLE 3 it is disclosed that the fields of interest for the filter can be selected and among the choices are the Destination MAC address and Source MAC address. Thus Sampath's Fast Filtering Processor (paragraph [0036]) can use the MAC address for filtering and determining whether to forward or discard packets); **and**

an IP filtering unit that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the destination MAC address and only

interface ID part of the source IPv6 address contained in the received packet (Paragraph [0014] of Sampath discloses that a packet is discarded, forwarded or modified based upon the filtering. Then in paragraphs [0051] and [0052] and TABLE 3 it is disclosed that the fields of interest for the filter can be selected and among the choices are the Destination MAC address and Source IP address. Thus Sampath's Fast Filtering Processor (paragraph [0036]) can use the IP address for filtering and determining whether to forward or discard packets).

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

35. **As to claim 15**, Sampath-Jouppi-Clark discloses the invention as claimed as described in claim 14,

**wherein the filtering processing unit of the network node device further comprises:
a filtering information storage unit for that stores at least the destination MAC address and the source MAC address or only the interface ID part of the source IPv6 address, and
judgment information representing relay or discard in association with each other**
(Paragraph [0039] of Sampath discloses the filter logic works by masking the portions of the packet that the filter is not interested in. Thus after masking is done a search key is generated that will be used to search for a match in the rules table. This rules table is seen to contain the destination MAC address and, source MAC address or source IPv6 address, because based on the

selections of fields F1 and F2 the rules table would then consist of the corresponding addresses. That is if F1 and F2 were assigned to be the Destination MAC address and the Source IP address respectively, then the search key would be composed of the Destination MAC address and the Source IP address. Then since the search key is used to match against the entries in the rules table, the rules table must contain the Destination MAC address and Source IP addresses also. As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that the rules table also contains the judgment information);

wherein the MAC filtering unit compares the destination MAC address and the source MAC address contained in the received packet with the destination MAC address and the source MAC address stored in the filtering information storage unit, and when the addresses match with each other, determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with the destination MAC address and the source MAC address (As Sampath disclosed above in claim 6 the filtering process involves masking the bits that are not relevant to the search and thus creating a search key that is composed of the fields chosen in the fields table. Thus if F1 and F2 were assigned to be the Destination MAC address and the Source MAC address respectively, the processor would be matching those against the entries in the rules tables (paragraph [0039]). As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if

the packet is discarded or sent to the CPU. Thus it is seen that if a match is found the results are taken from the rules table determining if the packet is discarded or forwarded), **and wherein the IP filtering unit compares destination MAC address and only the interface ID part of the source IPv6 address contained in the received packet with the destination MAC address and only the interface ID part of the source IPv6 address stored in the filtering information storage unit, and wherein when the addresses and interface ID parts match with each other, determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with the judgment information associated with the destination MAC address and only the interface ID part of the source IPv6 address** (As Sampath disclosed above in claim 6 the filtering process involves masking the bits that are not relevant to the search and thus creating a search key that is composed of the fields chosen in the fields table. Thus if F1 and F2 were assigned to be the Destination MAC address and the Source IP address respectively, the processor would be matching those against the entries in the rules tables (paragraph [0039]). As to the judgment information, paragraphs [0036] and [0037] disclose that the results are obtained from the rules table and that the outcome of the filtering logic decides if the packet is discarded or sent to the CPU. Thus it is seen that if a match is found the results are taken from the rules table determining if the packet is discarded or forwarded).

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

36. As to claim 16, Sampath discloses a network apparatus comprising:
plural network interface units connected with a network and that transmit/receive packets
(Paragraph [0022] of Sampath discloses Gigabit Port Interface Controller module interfaces which performs both the ingress and egress functions. This is seen to be a single unit connected to a network that transmits and receives. Then in figure 1 it is seen that there are multiples of them);
a packet relay unit that relays a received packet between the plural network interface units in accordance with a destination address of the received packet (Paragraph [0021] of Sampath discloses figure 1 being a switch on chip. Thus it is seen that the switch is an inherent part of the device and then in paragraph [0005] a switch is disclosed to be capable of switching a packet to an appropriate output port); **and**
a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet switch unit or discard the packet in accordance with;
one or more of a destination MAC address and the destination IPv6 address and the source MAC address; and
only the interface ID part of the source IPv6 address extracted from the received packet
(Paragraph [0014] of Sampath discloses running packets through a faster filtering processor to

obtain a selective filter action. The packets are discarded, forwarded or modified based upon the filtering. Then paragraph [0051] discloses a field table that specifies the fields of interest for the filter. The field table is clarified in paragraph [0052] to contain three portions which are described in TABLE 3. In TABLE 3 it is seen that fields F1 and F2 can be any of the Source MAC address, Destination MAC address, Source IP address and L4 Source Port, Destination IP address and L4 Port, or a user defined 16 bit field. These two fields are seen to be the same as those in applicant's invention. As to the IP addresses being IPv6, paragraph [0042] discloses the fields include Ethernet and IPv4 fields, as well as IPv6 field); and

Sampath does not explicitly disclose an authentication unit that executes authentication based on predetermined information received from an arbitrary information terminal device connected to one of the network interface units via the network.

However, Clark discloses this (Column 6 lines 15 – 25 of Clark disclose a user's authentication request being forwarded to an authentication server for processing. The authentication server then checks the user's ID and password received from the user with its own database. The user's ID and password are seen to be predetermined information related to the terminal device)

Examiner recites the same rationale to combine used in claim 8.

Sampath does not explicitly disclose wherein the filtering processing unit determines a condition for a determination of whether to relay or discard based on the authentication result by the authentication unit.

However, Clark discloses this (Figure 6A of Clark discloses a sample of a subscriber requesting information, as seen in step 614 the dynamic filtering firewall checks to see if the IP

address is marked as authenticated. If it is authenticated the communication is permitted and thus the packet would be forwarded)

Examiner recites the same rationale to combine used in claim 8.

Sampath does not explicitly disclose the portions pertaining to only the interface ID part of the source IPv6 address.

However, Jouppi discloses this (Paragraph [0030] of Jouppi discloses when a packet is received, its interface identifier is checked to determine whether or not to transmit the packet)

Examiner recites the same rationale to combine used in claim 1.

37. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sampath-Jouppi as applied to claim 1 above, and further in view of U.S. Pat. No. 7051365 to Bellovin (hereinafter "Bellovin").

38. **As to claim 10**, Sampath-Jouppi discloses the invention as claimed as described in claim 1. Sampath-Jouppi does not explicitly disclose **a security control unit that generates or exchanges a key for packet encryption or decoding for each communication counterpart, using a key exchange protocol; and a security processing unit for that executes authentication of at least the received packet, using the key generated by the security control unit.**

However, Bellovin discloses this (Column 8 lines 55 – 56 of Bellovin disclose a packet filter processor that operates in accordance with the IPSEC module. IPSEC is well known to deal with authentication and encryption of packets. Then column 10 lines 65 – 67 and column

11 lines 1 – 15 disclose the key exchange and certificate validation is performed using a public key cryptography algorithm. As to authenticating using the key, column 10 line 46 discloses the packet filter processor receiving a packet then in column 10 lines 55 - 65 it states when a packet is received, the header has a pointer to a data area containing a cryptographic key. The key is used to authenticate the packet by means of a cryptographic function as set forth in IPSEC).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the apparatus of claim 1 as disclosed by Sampath, with having a security unit for authenticating using a key as disclosed by Bellovin. One of ordinary skill at the time the invention was made would have been motivated to combine to add another layer of protection against unauthorized intrusions (column 2 lines 65 – 67 of Bellovin).

Conclusion

39. A shortened statutory period for reply to this Office action is set to expire THREE MONTHS from the mailing date of this action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN S. MAI whose telephone number is (571)270-5001. The examiner can normally be reached on Monday through Friday 7:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KSM
/Yasin M Barqadle/

Primary Examiner, Art Unit 2456